Quadratic Semigroups on Affine Spaces

Mohan S. Putcha
Department of Mathematics
North Carolina State University
Raleigh, North Carolina 27650

Submitted by Hans Schneider

ABSTRACT

As a generalization of some aspects of the theories of algebraic groups and finite dimensional algebras one can study polynomially defined, associative operations on affine spaces. In this paper we study the quadratic case—i.e., the case when the polynomials are of degree at most two. We call the resulting semigroup a quadratic semigroup. We obtain the complete structure for one class of quadratic semigroups and a representation theorem for another class.

1. PRELIMINARIES

Throughout this paper, $\mathbb{R}$, $\mathbb{C}$ will denote the sets of reals and complex numbers, respectively. F will denote an arbitrary field, t, and $t_1, t_2, \dots$ will denote variables. $F[t_1,\dots,t_n]$ will denote the polynomial ring in commuting variables $t_1,\dots,t_n$. $F^n = F\times\cdots\times F$ will denote the affine n-space, and $\mathfrak{M}_n(F)$ the algebra of all $n\times n$ matrices over F. Let $\mathcal{V}$ be a vector space over F. Then we let $\mathcal{L}(\mathcal{V})$ denote the algebra of all linear transformations from $\mathcal{V}$ into $\mathcal{V}$. If $A\in\mathcal{L}(\mathcal{V})$ and $X\in\mathcal{V}$, then we write AX for $A(X)$. If $A,B\in\mathcal{L}(\mathcal{V})$, then we write AB for the composition of A and B. We let I denote the identity transformation on $\mathcal{V}$. If $*$ is a binary operation on $\mathcal{V}$ and if $X,Y\in\mathcal{V}$, $A\in\mathcal{L}(\mathcal{V})$, then we write $AX*Y$ for $(AX)*Y$. A binary operation $*$ on $\mathcal{V}$ is *bilinear* if the corresponding map from $\mathcal{V}\times\mathcal{V}\to\mathcal{V}$ is bilinear. $*$ is *trivial* if $X*Y=0$ for all $X,Y\in\mathcal{V}$. If $*$ is an associative, bilinear operation on $\mathcal{V}$, then we say that $(\mathcal{V},*)$ is an *algebra*. Thus our algebras need not have identity elements. Let $(\mathcal{V},*)$ be an algebra. We can define a binary operation $\circ$ on $\mathcal{V}$ as $X\circ Y = X+Y+X*Y$. Following ring theorists, we refer to $(\mathcal{V},\circ)$ as the *circle semigroup* of the algebra $(\mathcal{V},*)$.

Let S be a semigroup, $u\in S$. Then u is a *right* [*left*] *zero* of S if $au=u$ [$ua=u$] for all $a\in S$. u is a *right* [*left*] *identity* of S if $au=a$ [$ua=a$] for all

 0024-3795/79/040107+15$01.75

$a \in S$. u is an *identity element* of S if u is both a right and a left identity of S. u is a *zero* of S if u is both a right and a left zero of S. Let T be a subsemigroup of S. Then S is an *inflation* of T if there exists a map $\phi: S \to T$ such that ϕ is the identity map on T and $ab = \phi(a)\phi(b)$ for all $a, b \in S$. The inflations of a semigroup T are obtained in purely set theoretic manner (cf. [3, p. 98, Exercise 10]). Let Γ be a set. Define $\circ$, $*$ on Γ as $a \circ b = b$, $a * b = a$, respectively. Then $(\Gamma, \circ)$ is called a *right zero semigroup* and $(\Gamma, *)$ a *left zero semigroup*. A direct product of a right zero semigroup and a left zero semigroup is called a *rectangular band*. The direct product of a right [left] zero semigroup and a group is called *right* [*left*] *group*. The direct product of a rectangular band and a group is called a *rectangular group*.

As a generalization of some aspects of the theories of algebraic groups and finite dimensional algebras, one can study polynomially defined associative operations on F^n. For $n = 1$, this has been done by Yoshida [8, 9] and by Plemmons and Yoshida [6]. Related papers are [2, 4, 7]. Yoshida's results have been generalized to infinite integral domains by Petrich [5]. In this paper we study associative operations on F^n defined by polynomials of degree at most 2.

Let $p_1(t_1, \ldots, t_{2n}), \ldots, p_n(t_1, \ldots, t_{2n}) \in F[t_1, \ldots, t_{2n}]$. Suppose each term of $p_i(t_1, \ldots, t_{2n})$ has length at most 2. If $X = (x_1, \ldots, x_n)$, $Y = (y_1, \ldots, y_n) \in F^n$, then let

$$X * Y = (p_1(x_1, \ldots, x_n, y_1, \ldots, y_n), \ldots,$$
$$\times p_n(x_1, \ldots, x_n, y_1, \ldots, y_n)).$$

We call $*$ a quadratic operation on F^n. It is easy to see that there exist $C \in F^n$, $A, B \in \mathcal{L}(F^n)$, and bilinear operations $\circ$, $\triangle$, $\square$ on F^n such that for all $X, Y \in F^n$,

$$X * Y = C + AX + BY + X \circ Y + X \triangle X + Y \square Y. \tag{1}$$

We will illustrate this with an example. Let $n = 2$, and suppose $(x_1, x_2) * (y_1, y_2) = (1 + x_1 + y_2 + x_1 y_2 + x_1^2 + x_1 x_2, 2 + 3x_2 + 5x_2 y_2 + x_2^2 + y_2^2)$. Then we can let $C = (1, 2)$, $A(x_1, x_2) = (x_1, 3x_2)$, $B(x_1, x_2) = (x_2, 0)$, $(x_1, x_2) \circ (y_1, y_2) = (x_1 y_2, 5x_2 y_2)$, $(x_1, x_2) \triangle (y_1, y_2) = (x_1 y_1 + x_1 y_2, x_2 y_2)$, $(x_1, x_2) \square (y_1, y_2) = (0, x_2 y_2)$.

Let $\mathcal{V}$ be a vector space over F. A binary operation $*$ on $\mathcal{V}$ is a *quadratic operation* if there exist $C \in \mathcal{V}$, $A, B \in \mathcal{L}(\mathcal{V})$, and bilinear operations $\circ$, $\triangle$, $\square$ on $\mathcal{V}$ such that (1) holds for all $X, Y \in \mathcal{V}$. Then

$$X \circ Y = X * Y - X * 0 - Y * 0 + 0 * 0.$$

Hence for a given $*$, $\circ$ is uniquely determined. Also, for all $X, Y, Z \in \mathcal{V}$,

$$\begin{aligned}(X\circ Y)\circ Z &= (X*Y)*Z-(X*Y)*0-(X*0)*Z\\ &\quad -(0*Y)*Z+(X*0)*0+(0*Y)*0\\ &\quad +(0*0)*Z-(0*0)*0,\\ X\circ(Y\circ Z) &= X*(Y*Z)-X*(Y*0)\\ &\quad -X*(0*Z)-0*(Y*Z)\\ &\quad +X*(0*0)+0*(Y*0)\\ &\quad +0*(0*Z)-0*(0*0).\end{aligned}$$

If $*$ is associative, we say that $(\mathcal{V}, *)$ is a *quadratic semigroup*. In such a case, by the above, $\circ$ is associative. Hence $(\mathcal{V}, \circ)$ is an algebra. We refer to $\circ$ as the *algebra part* of $*$ and $(\mathcal{V}, \circ)$ as the *algebra* of $*$. We define the *dimension* of $S=(\mathcal{V}, *)$ as being the dimension of $\mathcal{V}$ over F.

Let $*$ be a quadratic operation on $\mathcal{V}$ given by (1). If $\operatorname{ch} F\neq 2$, then $\triangle$, $\square$ can be chosen to be commutative. In fact,

$$X*Y=C+AX+BY+X\circ Y+X\theta_1 X+Y\theta_2 Y,$$

where

$$X\theta_1 Y=\tfrac{1}{2}(X\triangle Y+Y\triangle X),\qquad X\theta_2 Y=\tfrac{1}{2}(X\square Y+Y\square X).$$

2. SPECIAL QUADRATIC SEMIGROUPS

Let $\mathcal{V}$ be a vector space over F. A binary operation $*$ on $\mathcal{V}$ is a *special quadratic operation* (s.q. operation) if there exist $C\in\mathcal{V}$, $A,B\in\mathcal{L}(\mathcal{V})$, and a bilinear operation $\circ$ on $\mathcal{V}$ such that

$$X*Y=C+AX+BY+X\circ Y. \tag{2}$$

If $*$ is associative, then we say that $S=(\mathcal{V}, *)$ is a *special quadratic* *semigroup* (s.q. semigroup). Let $X, Y, Z \in \mathcal{V}$. Then by (2),

$$(X * Y) * Z = C + AC + A^2X + ABY + BZ + C \circ Z$$
$$+ A(X \circ Y) + AX \circ Z + BY \circ Z + (X \circ Y) \circ Z,$$
$$X * (Y * Z) = C + BC + AX + X \circ C + BAY + B^2Z$$
$$+ X \circ AY + X \circ BZ + B(Y \circ Z) + X \circ (Y \circ Z).$$

If $*$ is associative, then $(X * Y) * Z = X * (Y * Z)$ for all $X, Y, Z \in \mathcal{V}$. Letting $X, Y, Z = 0$, we see that $AC = BC$. Then letting $X = Z = 0$, we see that $AB = BA$. Continuing, we see that the following equations hold for all $X, Y, Z \in \mathcal{V}$:

$$AC = BC, \tag{3}$$
$$AB = BA, \tag{4}$$
$$(A^2 - A)X = X \circ C, \tag{5}$$
$$(B^2 - B)Z = C \circ Z, \tag{6}$$
$$A(X \circ Y) = X \circ AY, \tag{7}$$
$$B(Y \circ Z) = BY \circ Z, \tag{8}$$
$$AX \circ Z = X \circ BZ, \tag{9}$$
$$(X \circ Y) \circ Z = X \circ (Y \circ Z). \tag{10}$$

THEOREM 2.1. *Let $\mathcal{V}$ be a finite dimensional vector space over F, and $S = (\mathcal{V}, *)$ and s.q. semigroup. Then S has an idempotent.*

Proof. We prove by induction on $\dim \mathcal{V} = n$. Let $*$ be given by (2), and let $\mathcal{W} = \{X \mid X \in \mathcal{V}, (A - B)X = 0\}$. Then $\mathcal{W}$ is a subspace of $\mathcal{V}$. Let $X \in \mathcal{W}$. By (4), $(A - B)AX = A(A - B)X = 0$. So $AX \in W$. Similarly $BX \in \mathcal{W}$. So $\mathcal{W}$ is A- and B-invariant. Let $X, Y \in \mathcal{W}$. Then by (7), (8), (9), $A(X \circ Y) = X \circ AY = X \circ BY = AX \circ Y = BX \circ Y = B(X \circ Y)$. Hence $X \circ Y \in \mathcal{W}$. Thus $\mathcal{W}$ is a subalgebra of $(\mathcal{V}, \circ)$. Also, by (3), $C \in \mathcal{W}$. Hence $(\mathcal{W}, *)$ is an s.q. semigroup. If $\dim \mathcal{W} < n$, then $(\mathcal{W}, *)$ and hence S has an idempotent. So assume $\mathcal{V} = \mathcal{W}$.

Then $A = B$. Hence

$$A(X \circ Y) = X \circ AY = AX \circ Y.$$

Let $\mathcal{K} = \{L | L \in \mathcal{L}(\mathcal{V}),\ L(X \circ Y) = X \circ LY = (LX) \circ Y\}$. Clearly $A, I \in \mathcal{K}$ and $\mathcal{K}$ is a subalgebra of $\mathcal{L}(\mathcal{V})$. Hence

$$f(A) \in \mathcal{K} \qquad \text{for all} \quad f(t) \in F[t]. \tag{11}$$

Case 1. *$I - A$ is invertible.* By (11), $(I-A)^{-1} \in \mathcal{K}$. Let $X = (I-A)^{-1}C$. Then by (5),

$$\begin{aligned} X * X &= (I-A)^{-1}C * (I-A)^{-1}C \\ &= C + 2A(I-A)^{-1}C + (I-A)^{-1}C \circ (I-A)^{-1}C \\ &= C + 2A(I-A)^{-1}C + (I-A)^{-2}[C \circ C] \\ &= C + 2A(I-A)^{-1}C + (I-A)^{-2}(A^2 - A)C \\ &= X. \end{aligned}$$

Case 2. *$I - A$ is not invertible.* Let $\phi: V \to V$ be given by $\phi(X) = X + C$. ϕ, $*$ induce the following s.q. operation on $\mathcal{V}$:

$$\begin{aligned} X \vartriangle Y &= [X - C] * [Y - C] + C \\ &= C_1 + A_1 X + A_1 Y + X \circ Y, \end{aligned}$$

where $C_1 = (I-A)(2I-A)C$, $A_1 = 2A - A^2$. Then $\phi: S \cong (\mathcal{V}, \vartriangle)$. It suffices to show that $(\mathcal{V}, \vartriangle)$ has an idempotent. Let $\mathcal{U} = \{f(A)C_1 | f(t) \in F[t]\}$. Then $\mathcal{U}$ is an A_1-invariant subspace of $\mathcal{V}$ and $C_1 \in \mathcal{U}$. Let $h(A) = (I-A)(2I-A)$. So $C_1 = h(A)C$. Let $X, Y \in \mathcal{U}$. Then $X = f(A)C_1$, $Y = g(A)C_1$ for some $f(t), g(t) \in F[t]$. So by (11)

$$\begin{aligned} X \circ Y &= f(A)h(A)C \circ g(A)h(A)C \\ &= f(A)g(A)h(A)h(A)(C \circ C) \\ &= f(A)g(A)h(A)h(A)(A^2 - A)C \\ &= f(A)g(A)h(A)(A^2 - A)C_1. \end{aligned}$$

Hence $X \circ Y \in \mathcal{U}$. Thus $(\mathcal{U}, \triangle)$ is an s.q. semigroup. If $\dim \mathcal{U} < n$, then by the induction hypothesis, $(\mathcal{U}, \triangle)$ and hence $(\mathcal{V}, \triangle)$ has an idempotent. So assume $\mathcal{U} = \mathcal{V}$. Let $X \in \mathcal{V}$. Then $X = p(A)C_1$ for some $p(t) \in F[t]$. So $X = (I-A)p(A)(2I-A)C \in (I-A)\mathcal{V}$. Hence $(I-A)\mathcal{V} = \mathcal{V}$ and $I-A$ is invertible. This contradiction proves the theorem. ∎

Let $\mathcal{V}$ be a finite dimensional vector space over F, and let $(\mathcal{V}, *)$ be an s.q. semigroup where $*$ is given by (2). By Theorem 2.1, there exists $U \in \mathcal{V}$ such that $U * U = U$. Let $\phi: \mathcal{V} \to \mathcal{V}$ be given by $\phi(X) = X - U$. This induces the following operation on $\mathcal{V}$:

$$X \theta Y = (X+U) * (Y+U) - U$$

$$= A_1 X + B_1 Y + X \circ Y$$

where $A_1, B_1 \in \mathcal{L}(\mathcal{V})$ are given by $A_1(X) = AX + X \circ U$ and $B_1 X = BX + U \circ X$, respectively. Clearly $\phi: (\mathcal{V}, *) \cong (\mathcal{V}, \theta)$.

Thus, without loss of generality, we can assume that in (2), $C = 0$. Hence

$$X * Y = AX + BY + X \circ Y. \tag{12}$$

Then by (3), (4), (5), (6) we have

$$A^2 = A, \qquad B^2 = B, \qquad AB = BA. \tag{13}$$

Let $\mathcal{V}_1 = AB\mathcal{V}$, $\mathcal{V}_2 = (I-A)B\mathcal{V}$, $\mathcal{V}_3 = (I-B)A\mathcal{V}$, $\mathcal{V}_4(I-A)(I-B)\mathcal{V}$. By (13), $\mathcal{V} = \mathcal{V}_1 \oplus \mathcal{V}_2 \oplus \mathcal{V}_3 \oplus \mathcal{V}_4$. Let $X_i \in \mathcal{V}_i$, $i = 1,2,3,4$. Then $AX_1 = X_1$, $BX_1 = X_1$, $AX_2 = 0$, $BX_2 = X_2$, $BX_3 = 0$, $AX_3 = X_3$, $AX_4 = BX_4 = 0$. Let $X, Y \in \mathcal{V}$. Then $X = X_1 + X_2 + X_3 + X_4$, $Y = Y_1 + Y_2 + Y_3 + Y_4$, for some $X_i, Y_i \in \mathcal{V}_i$, $i = 1,2,3,4$. Then by (7), (8), (9), (13),

$$X * Y = Z_1 + Z_2 + Z_3 + Z_4, \tag{14}$$

where

$$\begin{aligned}
Z_1 &= X_1 \circ Y_1 + X_2 \circ Y_3 + X_1 + Y_1 \in \mathcal{V}_1, \\
Z_2 &= X_1 \circ Y_2 + X_2 \circ Y_4 + Y_2 \in \mathcal{V}_2, \\
Z_3 &= X_3 \circ Y_1 + X_4 \circ Y_3 + X_3 \in \mathcal{V}_3, \\
Z_4 &= X_3 \circ Y_2 + X_4 \circ Y_4 \in \mathcal{V}_4.
\end{aligned} \tag{15}$$

Also,

$$\mathcal{V}_1 \circ \mathcal{V}_1 + \mathcal{V}_2 \circ \mathcal{V}_3 \subseteq \mathcal{V}_1, \qquad \mathcal{V}_1 \circ \mathcal{V}_2 + \mathcal{V}_2 \circ \mathcal{V}_4 \subseteq \mathcal{V}_2,$$
$$\mathcal{V}_3 \circ \mathcal{V}_1 + \mathcal{V}_4 \circ \mathcal{V}_3 \subseteq \mathcal{V}_3, \qquad \mathcal{V}_3 \circ \mathcal{V}_2 + \mathcal{V}_4 \circ \mathcal{V}_4 \subseteq \mathcal{V}_4. \tag{16}$$

Let $\mathcal{Q} = (\mathcal{V}, \circ)$ be the algebra of $*$. Let $\mathfrak{M}_2(\mathcal{Q})$ denote the algebra of all 2×2 matrices over $\mathcal{Q}$. Let

$$\mathcal{U} = \left\{ \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix} \middle| X_i \in \mathcal{V}_i,\ i = 1,2,3,4 \right\}.$$

Then by (16), $\mathcal{U}$ is a subalgebra of $\mathfrak{M}_2(\mathcal{Q})$. If

$$\begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}, \begin{pmatrix} Y_1 & Y_2 \\ Y_3 & Y_4 \end{pmatrix} \in \mathcal{U},$$

then let

$$\begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix} \triangle \begin{pmatrix} Y_1 & Y_2 \\ Y_3 & Y_4 \end{pmatrix} = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}\begin{pmatrix} Y_1 & Y_2 \\ Y_3 & Y_4 \end{pmatrix} + \begin{pmatrix} X_1 + Y_1 & Y_2 \\ X_3 & 0 \end{pmatrix}.$$

Then $(\mathcal{U}, \triangle)$ is an s.q. semigroup. By (14), (15), $(\mathcal{V}, *) \cong (\mathcal{U}, \triangle)$, where $X = X_1 + X_2 + X_3 + X_4$, $X_i \in \mathcal{U}_i$, $i = 1,2,3,4$ corresponds to $\begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}$. We have thus proved the following structure theorem, which is similar in nature to the one obtained for matrix semigroups forming a linear variety by Clark [2].

THEOREM 2.2. *Let $\mathcal{Q}$ be a finite dimensional algebra over F, and $\mathfrak{M}_2(\mathcal{Q})$ the algebra of all 2×2 matrices over $\mathcal{Q}$. Suppose $\mathcal{V}_1, \mathcal{V}_2, \mathcal{V}_3, \mathcal{V}_4$ are subspaces of $\mathcal{Q}$, and*

$$\mathcal{U} = \left\{ \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix} \middle| X_i \in \mathcal{V}_i,\ i = 1,2,3,4 \right\}$$

is a subalgebra of $\mathfrak{M}_2(\mathcal{Q})$. Define an operation $\triangle$ on $\mathcal{U}$ as follows:

$$\begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix} \triangle \begin{pmatrix} Y_1 & Y_2 \\ Y_3 & Y_4 \end{pmatrix} = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}\begin{pmatrix} Y_1 & Y_2 \\ Y_3 & Y_4 \end{pmatrix} + \begin{pmatrix} X_1 + Y_1 & Y_2 \\ X_3 & 0 \end{pmatrix}. \tag{17}$$

Then $(\mathcal{U}, \triangle)$ *is an s.q. semigroup. Moreover, every finite dimensional s.q. semigroup over F is isomorphic to such a semigroup.*

Suppose $(\mathcal{V}, *)$ is commutative. Then clearly $A = B$ and $\mathcal{C} = (\mathcal{V}, \circ)$ is commutative. Hence $\mathcal{V}_2 = \mathcal{V}_3 = \{0\}$. By (16), $(\mathcal{V}_1, \circ)$ and $(\mathcal{V}_2, \circ)$ are subalgebras of $\mathcal{C}$. Hence we have the following

THEOREM 2.3. *Let* $\mathcal{C}_1$, $\mathcal{C}_2$ *be finite dimensional commutative algebras over F. Let* $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2$. *If* $X_1, Y_1 \in \mathcal{C}_1$, $X_2, Y_2 \in \mathcal{C}_2$, *then define*

$$(X_1, X_2) \triangle (Y_1, Y_2) = (X_1 Y_1 + X_1 + Y_1, X_2 + Y_2).$$

Then $(\mathcal{C}, \triangle)$ *is a commutative, s.q. semigroup. Moreover, every finite dimensional commutative, s.q. semigroup is isomorphic to such a semigroup.*

THEOREM 2.4. *Let* $S = (\mathcal{V}, *)$ *be a finite dimensional s.q. semigroup. Then S is isomorphic to a multiplicative subsemigroup of* $\mathcal{M}_p(F)$ *for some positive integer p.*

Proof. By Theorem 2.2, $S \cong (\mathcal{U}, \triangle)$, where $\mathcal{U}$ is as in Theorem 2.2. As is well known (cf. [1, p. 102, Theorem 8]), $\mathcal{C}$ is a subalgebra of $\mathcal{C}_1$ where $\mathcal{C}_1$ has an identity element 1. Define $\triangle$ on $\mathcal{M}_2(\mathcal{C}_1)$ by (17). Then $(\mathcal{U}, \triangle)$ is a subsemigroup of $S_1 = (\mathcal{M}_2(\mathcal{C}_1), \triangle)$. Let S_2 denote the multiplicative semigroup of $\mathcal{M}_2(\mathcal{C}_1)$. Then $\psi: S_1 \cong S_2$, where

$$\psi\begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix} = \begin{pmatrix} X_1 + 1 & X_2 \\ X_3 & X_4 \end{pmatrix}.$$

$\mathcal{M}_2(\mathcal{C}_1)$, being finite dimensional, is embeddable in $\mathcal{M}_p(F)$ for some positive integer p (cf. [1, p. 102, Theorem 8]). ∎

EXAMPLE 2.1. Let $S = (F^3, *)$, where

$$(x_1, x_2, x_3) * (y_1, y_2, y_3) = (x_2 y_3 + x_1 + y_1, y_2, x_3).$$

It is routinely verified that S is an s.q. semigroup. If $a, b \in S$, then $e = (-ab, a, b)$ is an idempotent. Let $H_{a,b} = \{(c, a, b) | c \in F\}$. Then $H_{a,b}$ is the maximal subgroup of e. $H_{0,0} \cong (F, +)$. Also $\phi: H_{a,b} \cong H_{0,0}$, where $\phi(c, a, b) = (ab + c, 0, 0)$. It is easily seen that S is a completely simple semigroup. If

$X=(x_1,x_2,x_3)\in S$, then let

$$\psi(X)=\begin{bmatrix}1 & x_2 & x_1\\ 0 & 0 & x_3\\ 0 & 0 & 1\end{bmatrix}.$$

Then ψ is an isomorphism from S into the multiplicative semigroup of $\mathfrak{M}_3(F)$.

REMARK 2.1. Clark [2] defines an "affine semigroup" to be a matrix semigroup forming a linear variety. By Theorems 2.2, 2.4, every finite dimensional s.q. semigroup is isomorphic to an "affine semigroup" (and conversely). However, we see no trivial proof of this fact.

3. QUADRATIC SEMIGROUPS

Let $S=(\mathcal{V},*)$ be a quadratic semigroup where $\mathcal{V}$ is a vector space over F. Then there exist $C\in\mathcal{V}$, $A,B\in\mathcal{L}(\mathcal{V})$, and bilinear operations $\circ$, $\triangle$, $\square$ on $\mathcal{V}$ such that for all $X,Y\in\mathcal{V}$

$$X*Y=C+AX+BY+X\circ Y+X\triangle X+Y\square Y. \tag{18}$$

If $W\in\mathcal{V}$, then we can define a new quadratic operation θ on $\mathcal{V}$ as

$$X\theta Y=(X+W)*(Y+W)-W.$$

Let $S_1=(\mathcal{V},\theta)$. Then $\psi:S\cong S_1$, where $\psi(X)=X-W$. We will say that θ is obtained by translating $*$ by W. Note that

$$X\theta Y=C_1+A_1X+B_1Y+X\circ Y+X\triangle X+Y\square Y, \tag{19}$$

where $C_1=(W*W)-W$, $A_1X=AX+X\circ W+X\triangle W+X\triangle W+W\triangle X$ and $B_1Y=BY+W\circ Y+Y\square W+W\square Y$. Clearly $A_1,B_1\in\mathcal{L}(\mathcal{V})$.

THEOREM 3.1. *Let $\mathcal{V}$ be a vector space over a field F and $S=(\mathcal{V},*)$ a quadratic semigroup.*

(1) *If S has an identity element, then S is isomorphic to the circle semigroup of the algebra of $*$.*

(2) *Suppose that there exist* $X_1, X_2 \in \mathcal{V}$ *such that* X_1 *is either a right identity or a right zero and* X_2 *is either a left identity or a left zero of* S. *Then* $*$ *is an s.q. operation.*

Proof. (1) Translating $*$ if necessary, we can assume that 0 is the identity of S. Since $0*0=C$, we see that $C=0$. Let $X \in \mathcal{V}$. Then $X=X*0=AX+X\triangle X$. Similarly $Y=Y\square Y+BY$. Hence $X*Y=X+Y+X\circ Y$.

(2) Translating $*$ if necessary, we can assume $X_1=0$. Then $0*0=C$. So $C=0$. If $X\in\mathcal{V}$, then $X*0=AX+X\triangle X$. Hence $\triangle$ can be chosen to be trivial. By (19) we see that $\triangle$ can be chosen to be trivial under any translation of $*$. Hence a dual argument shows that $\square$ can also be chosen to be trivial. ■

Suppose F is an infinite field. Let $f(t_1,\ldots,t_m)\in F[t_1,\ldots,t_m]$. Then, as is well known, $f(a_1,\ldots,a_m)=0$ for all $a_1,\ldots,a_m\in F$ implies $f\equiv 0$ (cf. [10; Chapter 1, § 18, Theorem 14]). We use this fact without further comment. For the rest of this section we assume that F is an *infinite field* of ch$\neq 2$. We further assume that the algebra part of $*$ is trivial. Thus

$$X*Y=C+AX+BY+X\triangle X+Y\square Y. \tag{20}$$

Since ch$F\neq 2$, we see as in Sec. 1 that $\triangle$, $\square$ can be chosen to be *commutative*. Suppose that $*$ is associative. Then

$$(X*Y)*Z=X*(Y*Z) \tag{21}$$

for all $X,Y,Z\in\mathcal{V}$. Let v_α $(\alpha\in\Omega)$ be a basis of $\mathcal{V}$. Let $X=\sum_{\alpha\in\Omega}x_\alpha v_\alpha$, $Y=\sum_{\alpha\in\Omega}y_\alpha v_\alpha$, $Z=\sum_{\alpha\in\Omega}z_\alpha v_\alpha$. Collecting together all expressions of the type $ax_ix_jy_ky_lv_\alpha(a\in F,\ i,j,k,l,\alpha\in\Omega)$, we obtain (since $\triangle$, $\square$ are bilinear) $2(X\triangle X)\triangle(Y\square Y)$ on the left side of (21). Such expressions do not appear on the right side of (21). Since F is an infinite field of ch$\neq 2$, we see that $(X\triangle X)\triangle(Y\square Y)=0$. Continuing this procedure, we see that (21) leads to the following equations:

$$AC+C\triangle C=BC+C\square C, \tag{22}$$

$$A^2X+2C\triangle AX=AX, \tag{23}$$

$$B^2Z+2C\square BZ=BZ, \tag{24}$$

$$ABY+2C\triangle BY=BAY+2C\square AY, \tag{25}$$

$$A(X\triangle X)+AX\triangle AX+2C\triangle(X\triangle X)=X\triangle X, \tag{26}$$

$$B(Z\square Z)+BZ\square BZ+2C\square(Z\square Z)=Z\square Z, \tag{27}$$

$$\begin{aligned}&A(Y\square Y)+2C\triangle(Y\square Y)+BY\triangle BY\\&\qquad=B(Y\triangle Y)+2C\square(Y\triangle Y)+AY\square AY,\end{aligned} \tag{28}$$

$$AX\triangle BY=0, \tag{29}$$

$$AY\square BZ=0, \tag{30}$$

$$(X\triangle X)\triangle(X\triangle X)=0, \tag{31}$$

$$(Z\square Z)\square(Z\square Z)=0, \tag{32}$$

$$(Y\triangle Y)\square(Z\square Z)=0, \tag{33}$$

$$(X\triangle X)\triangle(Y\square Y)=0, \tag{34}$$

$$(Y\square Y)\triangle(Y\square Y)=(Y\triangle Y)\square(Y\triangle Y), \tag{35}$$

$$(X\triangle X)\triangle AX=0, \tag{36}$$

$$BZ\square(Z\square Z)=0, \tag{37}$$

$$(Z\square Z)\square AY=0, \tag{38}$$

$$(Y\triangle Y)\square BZ=0, \tag{39}$$

$$(Y\triangle Y)\square AY=(Y\square Y)\triangle BY, \tag{40}$$

$$(X\triangle X)\triangle BY=0, \tag{41}$$

$$(Y\square Y)\triangle AX=0. \tag{42}$$

By (22),

$$AC\triangle AC+AC\triangle(C\triangle C)=AC\triangle BC+AC\triangle(C\square C).$$

So by (29), (36), (42),

$$AC\triangle AC=0. \tag{43}$$

Similarly by (22), (30), (37), (39),

$$BC\square BC = 0. \tag{44}$$

Also by (22),

$$AC\square AC + AC\square(C\triangle C) = AC\square BC + AC\square(C\square C).$$

Hence by (30), (38),

$$AC\square AC = -AC\square(C\triangle C). \tag{45}$$

Again by (22),

$$AC\square(C\triangle C) + (C\triangle C)\square(C\triangle C) = BC\square(C\triangle C) + (C\square C)\square(C\triangle C).$$

Thus by (33), (39),

$$(C\triangle C)\square(C\triangle C) = -AC\square(C\triangle C). \tag{46}$$

LEMMA 3.2. *Let* S *be a semigroup such that* $T = S^2$ *is a rectangular group. Suppose that for all* $a, b, c, d \in S$, $abcd = acbd$. *Suppose also that there exists an idempotent* e *of* S *such that* $aeb = ab$ *for* $a, b \in S$. *Then* S *is an inflation of* T.

Proof. Let $a \in S$. Then $eae \in G$, where G is the maximal subgroup of e. Let $\phi(a) = a(eae)^{-1}a$, where the inverse is taken in G. Clearly $\phi(S) \subseteq T$ and $\phi(a) = a$ for all $a \in T$. Let $a, b \in S$. Then

$$\begin{aligned}\phi(a)\phi(b) &= a(eae)^{-1}ab(ebe)^{-1}b\\ &= a(eae)^{-1}eab(ebe)^{-1}b\\ &= a(eae)^{-1}eaeebe(ebe)^{-1}b\\ &= aeb\\ &= ab.\end{aligned}$$

Hence S is an inflation of T. ∎

THEOREM 3.3. *Let $\mathcal{V}$ be a vector space over F such that F is an infinite field and* $\mathrm{ch}\, F \neq 2$. *Supose that $S=(\mathcal{V}, *)$ is a quadratic semigroup such that the algebra part of $*$ is trivial. Then S is an inflation of a rectangular group with the group being isomorphic to $(\mathcal{W}, +)$ for some subspace $\mathcal{W}$ of $\mathcal{V}$.*

Proof. Assume that $*$ is given by (20). Then Eqs. (22) to (46) must be valid. Let $W = C - 2AC - 2C \triangle C$. By (31), (36), (43),

$$AW + W \triangle W = AC - 2A^2C - 2A(C \triangle C) + C \triangle C$$

$$-4C \triangle AC - 4C \triangle (C \triangle C).$$

Hence by (23), (26), (43),

$$AW + W \triangle W = -AC - C \triangle C. \tag{47}$$

By (45), (46),

$$BW + W \square W = BC - 2BAC - 2B(C \triangle C)$$

$$+ C \square C - 4C \square AC - 4C \square (C \triangle C).$$

By (22),

$$BAC + B(C \triangle C) = B^2C + B(C \square C),$$

$$C \square AC + C \square (C \triangle C) = C \square BC + C \square (C \square C).$$

Hence

$$BW + W \square W = BC - 2B^2C - 2B(C \square C)$$

$$+ C \square C - 4C \square BC - 4C \square (C \square C).$$

So by (24), (27), (44)

$$BW + W \square W = -BC - C \square C. \tag{48}$$

It follows by (22), (47), (48) that $W * W = W$. Translating $*$ by W, if necessary, we can assume by (19) that $C = 0$. Then by (23), (24), (25),

$$A^2 = A, \qquad B^2 = B, \qquad AB = BA. \tag{49}$$

By (26), (31), (36), (49), we see that

$$X*0*Y=X*Y \qquad \text{for all} \quad X,Y\in\mathcal{V}. \tag{50}$$

Let $G=\{X|X\in S,\ X*0=X=0*X\}$. Then G is a subsemigroup of S with identity element 0. Let $X\in G$. Then

$$X=AX+X\triangle X \tag{51}$$

$$X=BX+X\square X. \tag{52}$$

By (29), (41), (51), $BX\triangle X=0$. So by (52), $X\triangle X=X\triangle(X\square X)$. Hence by (34), (42), (51), $X\triangle X=0$. Similarly $X\square X=0$. Hence $G=\{X|X\in S,\ X=AX=BX,\ X\triangle X=X\square X=0\}$. So for all $X,Y\in G$, $X+Y=X*Y\in G$. Let $\alpha\in F$, $X\in G$. Then $\alpha X=A\alpha X=B\alpha X$, $\alpha X\triangle\alpha X=\alpha^2(X\triangle X)=0$, $\alpha X\square\alpha X=0$. Hence $\alpha X\in G$. Thus G is also a subspace of $\mathcal{V}$ and $(G,+)=(G,*)$. Let $T=S^2$. We claim that T is a union of groups. Let $M\in T$. Then $M=X*Y$ for some $X,Y\in S$. Now $W=0*Y*X*Y*0\in G$. So there exists $Z\in G$ such that $W*Z=0$. By (50), $M^2*N=M$, where $N=Z*Y\in T$. Similarly there exists $N_1\in T$ such that $N_1*M^2=M$. By a theorem of Croisot (cf. [3, Theorem 4.3]) T is a union of groups. Let $X\in S$ such that $X*X=X$. Then

$$X=AX+BX+X\triangle X+X\square X. \tag{53}$$

So by (30), (32), (33), (37), (38), (39)

$$\begin{aligned} X\square X=&AX\square AX+2AX\square(X\triangle X)\\ &+(X\triangle X)\square(X\triangle X)+BX\square BX. \end{aligned}\tag{54}$$

Applying B to (53) and using (49), we obtain

$$BAX+B(X\triangle X)+B(X\square X)=0. \tag{55}$$

Now $X*0=AX+X\triangle X$. So we see by (27), (54), (55) that $0*X*0=0$. Let $X,Y\in S$ such that $X^2=X$, $Y^2=Y$. Then $0*X*0=0=0*Y*0$. So by (50),

$$X*Y*X=X*0*Y*0*X=X*0*X=X*X=X.$$

Hence [3, p. 83, Exercise 8] the idempotents of T form a rectangular band. By a theorem of Clifford (cf. [3; Theorem 4.6]), T is a rectangular group. Let $X,Y\in S$. Then $0*X*0, 0*Y*0\in G$. Thus by (50), $0*X*Y*0=0*X*0*0*Y*0=0*Y*0*0*X*0=0*Y*X*0$. Hence by (50),

$K*X*Y*M=K*Y*X*M$ for all $X, Y, K, M \in S$. By Lemma 3.2, S is an inflation of T. This proves the theorem. ■

EXAMPLE 3.1. Let $\mathcal{V}=F^2$, and let $*$ be the quadratic operation on $\mathcal{V}$ defined by

$$(x_1, x_2)*(y_1, y_2)=(x_1, x_2+y_2+y_1^2).$$

Then it is routinely verified that $S=(\mathcal{V}, *)$ is a quadratic semigroup. The maximal subgroup of $(0,0)$ is $\{(0,x)|x\in F\}\cong(F,+)$. It can also be seen that S is a left group.

Finally the author would like to thank Professor Boris Schein for a number of very valuable suggestions.

REFERENCES

1 A. Abian, *Linear Associative Algebras*, Pergamon, 1971.
2 W. E. Clark, Affine semigroups over an arbitrary field, *Proc. Glasgow Math. Assoc.* 7:80–92 (1965).
3 A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups*, Vol. 1, Amer. Math. Soc., Providence, R.I., 1961.
4 H. Cohen and H. S. Collins, Affine semigroups, *Trans. Amer. Math. Soc.* 93:97–113 (1959).
5 M. Petrich, Associative polynomial multiplications over an integral domain, *Math. Nachr.* 29:67–75 (1965).
6 R. J. Plemmons and R. Yoshida, Generating polynomials for finite semigroups, *Math. Nachr.* 47:69–75 (1970).
7 D. C. Ramsey, Generating monomials for finite semigroups, *Pacific J. Math.* 39:783–794 (1971).
8 R. Yoshida, Algebraic systems which admit polynomial operations, *Mem. Res. Inst. Sci. Eng. Ritsumeikan Univ.* 10:1–5 (1963).
9 R. Yoshida, On some semigroups, *Bull. Amer. Math. Soc.* 69:369–371 (1963).
10 O. Zariski and P. Samuel, *Commutative Algebra*, Vol. 1, Van Nostrand, 1958.

Received 17 March 1978; revised 23 October 1978